Groupe SCOPELEC

RGPD

Appréhender la démarche de mise en conformité RGPD pour vos entreprises.

RGPD

En français: **RGPD**: **R**èglement **G**énéral à la **P**rotection des **D**onnées
En anglais: **GDPR**: **G**eneral **D**ata **P**rotection **R**egulation

Il s'agit d'une règlementation européenne visant à renforcer la protection des données personnelles de l'ensemble des citoyens européen.

✓ Objectif: Redonner aux Citoyens le contrôle sur leurs données personnelles.

ENTREE EN VIGUEUR:

Loi informati[illegible]e et Libertés

Groupe SCOPELEC
La performance collective

RGPD

En bref…

99

Articles

11

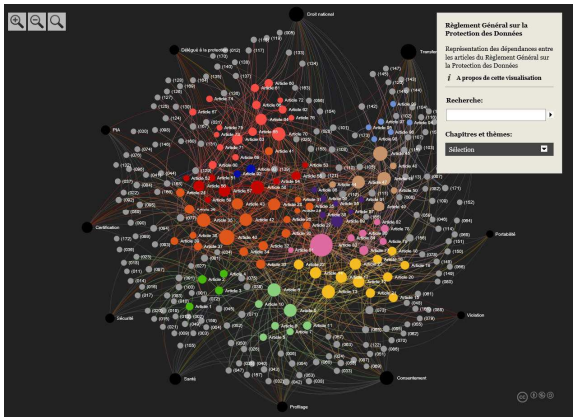
Chapitres

173

« Considérants »

≃200

Pages



Dataviz

1 (Article 32)

Parlant de Technologie

Donnée personnelle

Définition: Une Donnée personnelle ou à caractère personnel est une Donnée qui permet de caractériser/identifier une personne physique.

Donnée personnelle

Nom / Prénom

Date de Naissance

Adresse postale

Identifiant d'équipement électronique

Information médias sociaux

Photographies

Collecte de données IoT

Adresse mail

Donnée personnelle sensible

Origine raciale ou ethnique

Orientations et préférences sexuelles

Opinions politiques, philosophiques ou religieuses

Adhésion syndicale

Santé

Donnée génétique / Biométrique

Séquences génétiques

Empreintes digitales

Reconnaissance faciale

Scan rétiniens

Le RGPD…

A qui s’applique t-il ?

RGPD

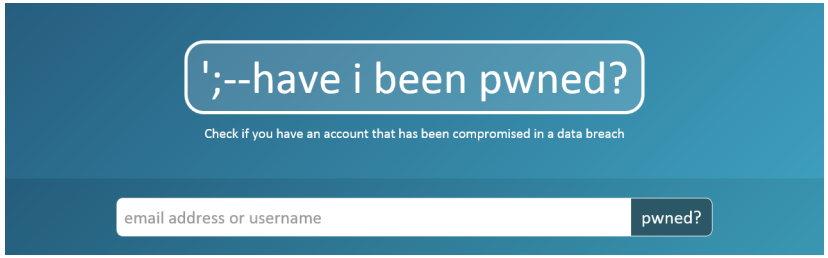
Le RGPD s'applique à tous les organismes traitant de données personnelles appartenant à des citoyens de l'**U**nion **E**uropéenne, c'est-à-dire:

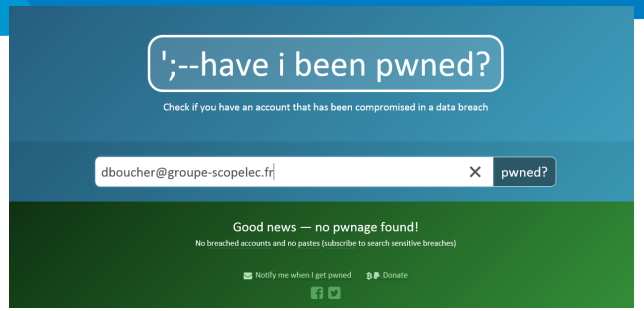
- ✓ les acteurs économiques et sociaux européens (entreprises, associations, administrations, collectivités locales, syndicats d'entreprise)
- ✓ les sous-traitants
- ✓ les entreprises hors Union Européenne qui proposent des services et biens sur le marché européen

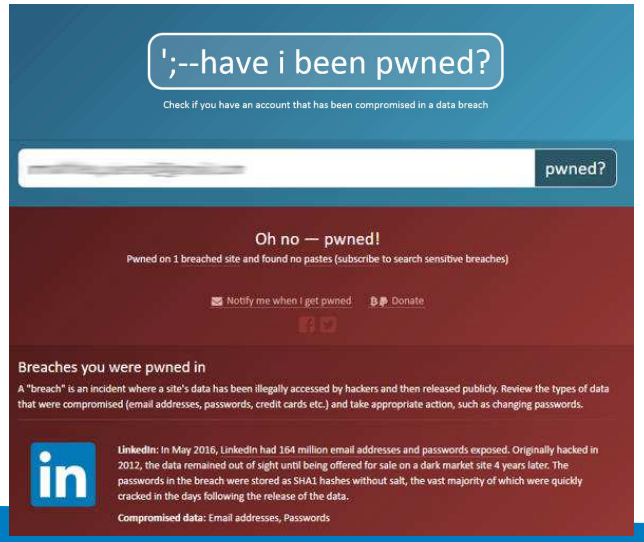
Faites le test...

Vérifiez si vos données ont été piratées

Le site « **Have I been pwned** » vérifie si votre email est concerné par l'une des Cyberattaques recensées par le site et ayant pu engendrer la violation de vos données personnelles.







Groupe SCOPELEC
La performance collective

Quels sont les devoirs de l'Entreprise en cas de fuite ou de violations des données personnelles ?

- ✓ En référer à la CNIL (autorité de contrôle pour la France) dans les 72h00 (Article 33)
- ✓ Notifier obligatoirement les incidents de sécurité ainsi que les atteintes aux Salariés de l'Entreprise en lui apportant les explications nécessaires.
- ✓ Apporter une remédiation.

Que se passe t-il en cas de non-conformité du Règlement ?

Sanctions

20 millions €

4%

CA

Effets collatéraux:

- ✓ Poursuites judiciaires
- ✓ Vols de données Business
- ✓ Perte de parts de marchés
- ✓ Dégâts pour l'image de marque

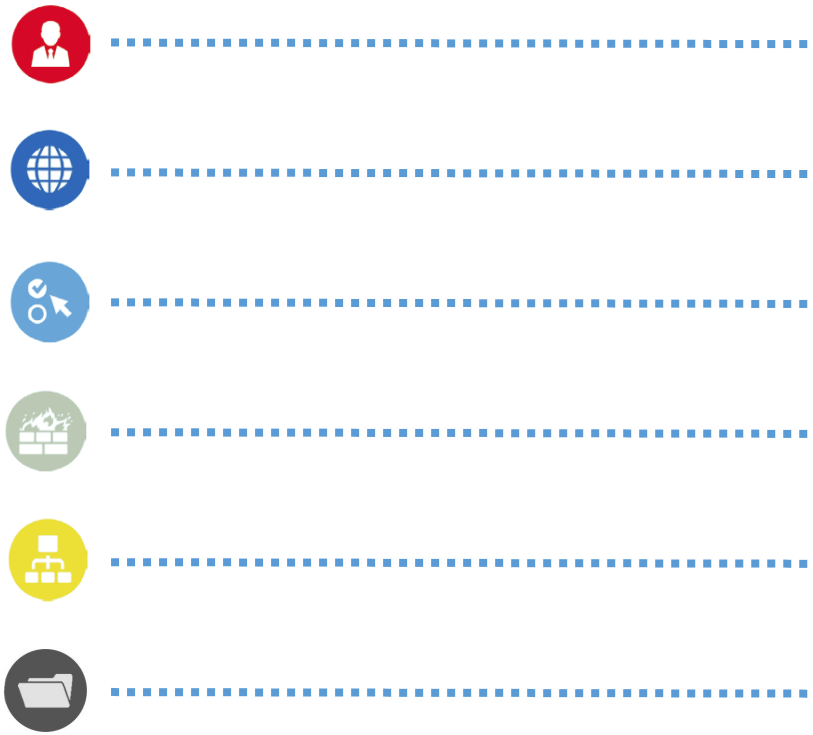
Le montant le plus élevé étant retenu.

Après la théorie…

La mise en œuvre…

Se préparer en 6 étapes

CNIL.



ETAPE 1
DESIGNER UN PILOTE

ETAPE 2
CARTOGRAPHIER LES TRAITEMENTS DE DONNEES PERSONNELLES

ETAPE 3
PRIORISER LES ACTIONS

ETAPE 4
GERER LES RISQUES

ETAPE 5
ORGANISER LES PROCESSUS INTERNES

ETAPE 6
DOCUMENTER LA CONFORMITE

Groupe SCOPELEC
La performance collective

RGPD

ETAPE 1: Désigner un pilote

1. Formation au DPO, DSI, RSSI, Responsable Qualité et Conformité

2. Formation/Sensibilisation en CODIR par un Avocat

3. Formation aux Services / Tronc commun + Adaptation métier (Services RH, Juridique, Marketing, Commercial,…)

En continu

RGPD

ETAPE 2: Cartographier vos traitements de données personnelles (1/2)

1. Cartographie des Traitements via des ITW métier:
   - ✓ De quelles données on dispose?
   - ✓ Quel est la finalité du traitement?
   - ✓ Quels sont les acteurs (internes ou externes) qui traitent les données?
   - ✓ Où sont-elles stockées?
   - ✓ Comment sont-elles sécurisées?
   - ✓ Quels sont les règles d'accès?
   - ✓ Quel est leur cycle de vie (historique, suppression, portabilité,…)

   → Mise en place d'un registre des activités des traitements.

   → Taguer les Données sensibles (→ EIVP)

RGPD

ETAPE 2: Cartographier vos traitements de données personnelles (2/2)

2. La Cartographie des risques sur les Données à caractère personnel (Macro)

3. L'identification des non-conformités:
   - ✓ Revue documentaire (charte informatique, PSSI, politique d'archivage des données, formulaires de consentement,…)
   - ✓ Evaluations de la conformité au RGPD

PLAN D'ACTION

RGPD

ETAPE 3: Prioriser les actions

Priorisation et identification des actions à mener pour se conformer aux obligations actuelles et à venir:

- → Court terme
- → Moyen terme
- → Long terme

RGPD

ETAPE 4: Gérer les risques

En français: **EIVP**: **E**tude d'**I**mpact sur la **V**ie **P**rivée
En anglais: **PIA**: **P**rivacy **I**mpact **A**ssessment
Relatif à la protection des données et obligatoire pour les traitements les plus risqués.
→ En fonction de la Cartographie des risques vue lors de l'Etape 2

2. Mise en œuvre:
   - Organisationnelle (Désignation des RT,…)
   - Juridique (Validation des documents,…)
   - Des solutions Techniques (Chiffrement, Droits d'accès, Supervision, Sauvegarde, Traçage des accès…)

RGPD

ETAPE 5: Organiser les processus internes (1/3)

1. **<u>Accompagnements</u>**:

- **Consultant Sécurité**

→ Chef de Projet Sécurité: Cartographie des risques, EIVP, consentements,…

- **Juriste**

→ C'est le rédacteur. Il analyse les Contrats SST, Clients, Travail, les CGV, CGU.

- **Avocat**

→ Le Valideur du plan d'action. Peut intervenir en cas de contrôle de la CNIL.

ETAPE 5: Organiser les processus internes (2/3)

2. **Recueil du consentement**: Elément-clé de la conformité des traitements mis en œuvre puisqu'il s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement portant sur leurs données personnelles.

Remarques:

- 1 finalité de traitement = 1 consentement
- 1 seul consentement est nécessaire si plusieurs traitements ont la même finalité.

→ On ne peut donc pas demander un consentement pour un but trop large, trop vague.

ETAPE 5: Organiser les processus internes (3/3)

Formes du consentement

CONSENTEMENT VALIDE

- Case à cocher (non pré-cochée)
- Déclaration (ex: formulaire papier) ou comportement indiquant clairement que la personne concernée accepte le traitement proposé.

RGPD

ETAPE 6: Documenter la conformité

Accountability: Désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

- ✓ Prouver ce que l'on met en place.
- ✓ Formaliser les procédures.

Combien de temps pour sa mise en œuvre ?

RGPD

- Taille de l'entreprise:

- Complexité du Système d'Information
- Secteur d'activité: (Privé, Public, Banque, Assurance, Retails)
- Sensibilité des Données: Santé, Bancaires,…

- Démarche interne: CIL
- Nombre de personne:
  - Gouvernance
  - Opérationnel
  - Juridique

- Temps consacré:
  - A plein temps
  - A temps partiel

Quel Budget pour sa mise en œuvre ?

RGPD

- Sensibilisations / Formations: ETAPE 1 (DPO, RT, Nombre d'utilisateurs gérant de la Donnée à caractère personnel)

- Accompagnement à la mise conformité:
  - Consultant Sécurité
  - Juriste
  - Avocat

  } Temps consacré (Nombre de jours)

- Niveau de sécurité souhaité:
  - Type d'outils
  - Processus internes (système automatisé ou manuel)

Pour aller plus loin…

Obligation de respecter les principes de protection des données suivants :

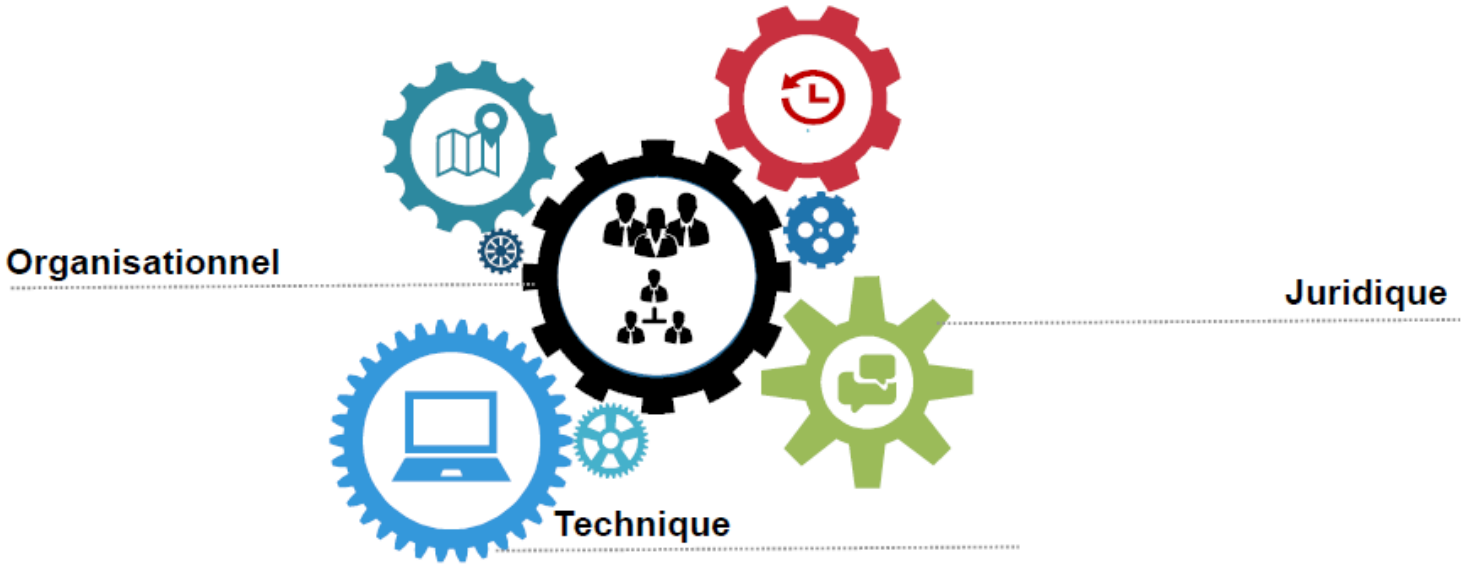
✓ **Privacy by design** « Protection de la vie privée dès la conception »
Nouveaux services, nouveaux produits,…
→ S'assurer que tout ce qui peut avoir un rapport avec le traitement de données à caractère personnel est bien conforme à la règlementation.

✓ **Privacy by default** « Protection de la vie privée par défaut »
→ Protéger les données à caractère personnel.

✓ **Security by design**
→ Gérer la sécurité d'un point de vue général.

Conclusion

C’est un Projet qui doit s’appréhender dans ces 3 dimensions



Mon argent ?
J'en prends soin.
Ma vie privée,
aussi.

CNIL.

Merci pour votre attention.

Groupe SCOPELEC

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

David BOUCHER
Responsable **S**écurité du **S**ystème d'**I**nformation / DPO
dboucher@groupe-scopelec.fr / 06.83.81.99.67
CESIN

Groupe SCOPELEC
La performance collective